Wiltshire Police
How to spot a Phishing email

This document will show you simple ways to identify a **PHISHING** email from a cybercriminal. **PHISHING** is the fraudulent practice of sending emails purporting to be from reputable companies in order to persuade individuals to reveal personal information, such as passwords and credit card numbers. These emails can come in many guises and for the most part are untargeted. The criminal doesn't care whether the victim is from a large organisation, SME, charity, school or individual; they are simply looking for an easy target.

SPEAR PHISHING is exactly the same process as a **PHISHING** email, except it is targeted to a specific individual or organisation. In these cases the email will purport to be a friend, family member or colleague.

For advice on how to spot both **PHISHING** and **SPEAR PHISHING** emails please read the different methods below.

Look at the sender's name and email address. Does it sound legitimate, or is it trying to mimic someone you know or a provider you may use?

Is it addressed to you by name, or does it refer to 'valued customer', or 'friend', or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.
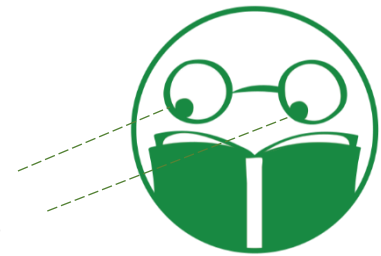
Read the email carefully, many phishing emails have poor grammar, punctuation and spelling - it may seem to have been poorly translated.

Does the email contain a veiled threat that asks you to act urgently? Be suspicious of phrases like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'. Take your time and don't be rushed by these calls to action.

Your bank, or any other official source, should never ask you to supply personal information from an email. This includes getting you to login to your account (!) or click a malicious link which could cause your device to be infected with Malware. If in doubt try calling them directly via an official number to ask if it's legitimate.

If you spot or fall victim to a PHISHING email please report it to Action Fraud (the national reporting centre for Cybercrime) and your employer if this occurs on work email address or device.

Phone: **0300 123 2040**
Website:
https://www.actionfraud.police.uk/

Created by Kieran Hall

Cyber Prevent & Protect Officers, DIIU